Amendment to the Specification:

Please replace the paragraph beginning at page 1, under the Related Applications section, with the following amended paragraph:

This application is a continuation in part of US Patent Application No.[[_____]] 09/758,941, filed January 10, 2001 and entitled "Mobile Application Security System and Method" which is a continuation in part of US Patent Application No. 09/645,028, filed August 23, 2000 and entitled "Mobile Application Security System and Method" which is a continuation in part of US Patent Application No. 09/591,034, filed June 9, 2000 and entitled "Mobile Application Security System and Method". All of the related applications are owned by the same assignee as the present invention.

Please replace the paragraph beginning at page 3, line 19 with the following amended paragraph:

A Trusted Computing Base (TCB) is the collection of computers, computer peripherals, and communication networks which must perform all requested operations properly, and must not perform extraneous operations, and are trusted to do so, in order to properly complete whatever computations are required.[[.]] A host outside of the TCB can perform nefarious tasks on the mobile application. This nefarious behavior cannot be controlled, and it cannot be detected. Therefore, once a mobile application has visited an untrusted host, it could be altered in an undesirable way, and therefore is a security hazard. In addition, the mobile application that visited the untrusted host can no longer be trusted to execute within the TCB. All of these security problems with mobile application need to be overcome before mobile applications become more accepted as [[a]] an alternative to traditional computing systems. Thus, it is desirable to provide a mobile application security system and method that overcomes the above problems and limitations with conventional mobile application systems and it is to this end that the present invention is directed so that mobile applications may be used in most financial, commercial, and military computer systems.

Please replace the paragraph beginning at page 12, line 10 with the following amended paragraph:

In a preferred embodiment, the mobile application controller 64 may include security software 66 and a communications software 68. The combination of the software may solve the problems with typical mobile application systems so that: 1) ~~An~~ A hostile host cannot send code with undesirable behavior to another host; 2) A mobile application can be protected from a hostile host; and 3) A mobile application can be securely sent to or received from a host outside of a group of trusted computers, known as the Trusted Computing Base (TCB) without fear of hostile activity. The way in which the security system in accordance with the invention overcomes these problems will now be described.

Please replace the paragraph beginning at page 30, line 4 with the following amended paragraph:

In this embodiment, a mobile application would typically move directly from node to node as in a peer-to-peer system. However, in accordance with the invention, on arrival at a node, the receiving host would inspect the arriving mobile application and send information about the arriving mobile application to the central security enforcement node 104. The CSEN could save the security information for future security checks. Then, the receiving node and the CSEN 104 may collectively perform different security procedures as described above to ensure that the mobile application is secure in the different manners described above. The CSEN 104 may have a similar ~~functionality~~ functionality and structure to the server 52 shown in Figure 4.